Successive Secret Key Agreement over Generalized Multiple Access and Broadcast Channels

Somayeh Salimi, Mikael Skoglund
ACCESS Linnaeus Center
School of Electrical Engineering, KTH
Stockholm, Sweden
somayen@kth.se, skoglund@ee.kth.se

Mahmoud Salmasizadeh
Electronics Research Center
Sharif University of Technology
Tehran, Iran
salmasi@sharif.edu

Mohammad Reza Aref
ISSL Lab., Dept. of Electrical Engineering
Sharif University of Technology
Tehran, Iran
aref@sharif.edu

arXiv:1202.1387v1 [cs.IT] 7 Feb 2012

***Abstract*—A secret key agreement framework between three users is considered in which each of the users 1 and 2 intends to share a secret key with user 3 and users 1 and 2 are eavesdroppers with respect to each other. There is a generalized discrete memoryless multiple access channel (GDMMAC) from users 1 and 2 to user 3 where the three users receive outputs from the channel. Furthermore, there is a broadcast channel (BC) from user 3 to users 1 and 2. Secret key sharing is intended where GDMMAC and BC can be successively used. In this framework, an inner bound of the secret key capacity region is derived. Moreover, for a special case where the channel inputs and outputs of the GDMAC and the BC form Markov chains in some order, the secret key capacity region is derived. Also the results are discussed through a binary example.**

I. Introduction

Ahlswede and Csiszar [1] and Maurer [2] introduced the problem of secret key sharing across the broadcast channel where, in addition to the broadcast channel, there is a noiseless public channel for communication between the transmitter and the receiver through which, all communications can be overheard by the eavesdropper. Secret key sharing over a pair of broadcast channels between two legitimate users in the presence of an eavesdropper was investigated in [4]. Furthermore, secrecy has been investigated in other frameworks where a user can be a legitimate user and simultaneously an eavesdropper. The broadcast channel with two confidential messages is investigated in [9] in which the transmitter intends to send independent confidential messages to two receivers where the receivers are eavesdroppers of each other's message. The generalized multiple access channel with two confidential messages was investigated in [5] where each of the two transmitters intends to send his message to the receiver and at the same time obtains information about the other transmitter's message through the received output from the channel. Secret key sharing over generalized multiple access channel has been investigated in [6] and [7] where each of the two transmitters wishes to share a secret key with the receiver while keeping it concealed from the other transmitter. In [6], there is a nioseless public channel from the transmitters to the receiver in addition to the generalized multiple access channel. In [7], there is a noiseless public channel from the receiver to the transmitters in such a way that the transmitters send information to the receiver through the generalized multiple access channel and the receiver communicates with the transmitters via the public channel.

We consider secret key sharing in a framework similar to [7] but in more conformity with real communication scenarios. There is a generalized discrete memoryless multiple access channel (GDMMAC) in the forward direction from users 1 and 2 to user 3 where in addition to user 3, the other users receive noisy outputs from the channel. Furthermore, instead of a public channel from user 3 to users 1 and 2 as in [7], there is a broadcast channel (BC) in the backward direction from user 3 to users 1 and 2. In this framework, users 1 and 2 intend to share secret keys with user 3 while users 1 and 2 are eavesdroppers with respect to each other. Users 1 and 2 send information to user 3 over the GDMMAC in the forward direction and user 3 answers them over the BC in the backward direction. The BC in the backward direction is used by user 3 to send feedback from the received output from the GDMMAC and also the inherent secrecy of the BC increases the secret key rates. This framework can be realized in a wireless network where users 1 and 2, as network users, can communicate with user 3, as a base station, through uplink (GDMMAC) and user 3 can communication with them through downlink (BC) and each of the network useres wishes to share a secret key with the base station hidden from the other user. We have derived an inner bound of the secret key capacity region. For a special case where the channel inputs and outputs of the GDMMAC and the BC form Markov chains in some orders, the secret key capacity region is obtained. Also a binary example is introduced and the bilateral effect of increasing the channel noise from user 3 to user 1 in the backward direction on the secret key capacity region is discussed.

The paper is organized as follows: in Section II, the preliminaries of our secret key framework are given. An inner bound of the secret key capacity region is given in Sections III. The secret key capacity for a special case and a binary example are presented in Section IV. The paper is concluded in Section V. Proofs of the results are presented in Appendices. In the paper, a random variable is denoted by an upper case letter and its realization is denoted by the corresponding lower case letter. We use X_i^N to indicate vector $(X_{i,1}, X_{i,2}, ..., X_{i,N})$, and $X_{i,j}^k$ to indicate vector $(X_{i,j}, X_{i,j+1}, ..., X_{i,k})$, where i denotes the index of the corresponding user.

II. Preliminaries

Users 1, 2 and 3 communicate over a pair of noisy channels. There is a GDMMAC in the forward direction from users 1 and 2 to user 3 and a BC from user 3 to users 1 and 2 in the backward direction. In the forward direction, users 1 and 2 govern inputs X_{1f} and X_{2f} of the GDMMAC with probability distribution $P_{Y_{1f},Y_{2f},Y_{3f}|X_{1f},X_{2f}}$, and outputs Y_{1f}, Y_{2f} and Y_{3f} are seen by users 1, 2 and 3, respectively. In the backward direction, user 3 governs input X_{3b} of the BC with probability distribution $P_{Y_{1b},Y_{2b}|X_{3b}}$, and outputs Y_{1b} and Y_{2b} are seen by users 1 and 2, respectively. Users 1 and 2 intend to share secret keys with user 3 where user 1 is the eavesdropper of user 2's key and vice versa. For simplicity, it is assumed that, like in [5], each transmitter uses the channel outputs to eavesdrop and not as inputs to the encoder when using the GDMMAC. Our results can be easily generalized to the situation where the channel outputs at the transmitters are used as inputs to the encoders of the GDMMAC as in [10], however it is beyond the scope of the present work. We represent the formal definition of the described secret key sharing as shown in Fig.1.

Step 1) n_f uses of the GDMMAC: Users 1 and 2 randomly generate independent keys K_{1f} and K_{2f}, respectively, and determine the i-th channel inputs $X_{1f,i}$ and $X_{2f,i}$ to the GDMMAC for $i = 1, 2, ..., n_f$ as stochastic mappings of the corresponding keys. Subsequently, the outputs $Y_{1f,i}, Y_{2f,i}$ and $Y_{3f,i}$ are observed by users 1, 2 and 3, respectively. User 3 estimates keys $\hat{K}_{1f}$ and $\hat{K}_{2f}$ as deterministic function of $Y_{3f}^{n_f}$.

Step 2) n_b uses of the BC: User 3 generates keys K_{1b} and K_{2b}, as stochastic functions of $Y_{3f}^{n_f}$ to share with users 1 and 2, respectively, and then, determines the i-th channel input $X_{3b,i}$ to the BC for $i = 1, 2, ..., n_b$ as a stochastic mapping of $Y_{3f}^{n_f}$. By receiving $Y_{1b}^{n_b}$ and $Y_{2b}^{n_b}$ over the BC by users 1 and 2, estimates $\hat{K}_{1b}$ and $\hat{K}_{2b}$ are produced by the corresponding users.

After these steps, the key pair (K_{1f}, K_{1b}) is shared between user 1 and user 3 and the key pair (K_{2f}, K_{2b}) is shared between user 2 and user 3. All the above keys take values in some finite sets. Now, we state the conditions that should be met in the described secret key sharing framework.

Definition 1: In the secret key sharing of the proposed model, the rate pair (R_1, R_2) is an achievable key rate pair if for every $\varepsilon > 0$ and sufficiently large n_f and n_b, we have:

$$\frac{1}{n_f+n_b} H(K_{1f}, K_{1b}) > R_1 - \varepsilon, \frac{1}{n_f+n_b} H(K_{2f}, K_{2b}) > R_2 - \varepsilon \quad (1)$$

$$\Pr\{(K_{1f},K_{1b}) \neq (\hat{K}_{1f},\hat{K}_{1b})\} < \varepsilon, \Pr\{(K_{2f},K_{2b}) \neq (\hat{K}_{2f},\hat{K}_{2b})\} < \varepsilon \quad (2)$$

$$\frac{1}{n_f+n_b} I(K_{1f}, K_{1b}; K_{2f}, X_{2f}^{n_f}, Y_{2f}^{n_f}, Y_{2b}^{n_b}) < \varepsilon \quad (3)$$

$$\frac{1}{n_f+n_b} I(K_{2f}, K_{2b}; K_{1f}, X_{1f}^{n_f}, Y_{1f}^{n_f}, Y_{1b}^{n_b}) < \varepsilon. \quad (4)$$

Equation (1) means that the rates R_1 and R_2 are the rates of the secret keys between user 1 and user 3 and user 2 and user 3, respectively. Equation (2) means that each user can correctly estimate the related keys. Equations (3) and (4) mean that users 1 and 2 effectively have no information about each other's secret keys.

Definition 2: The region containing all achievable secret key rate pairs (R_1, R_2) is the secret key capacity region.

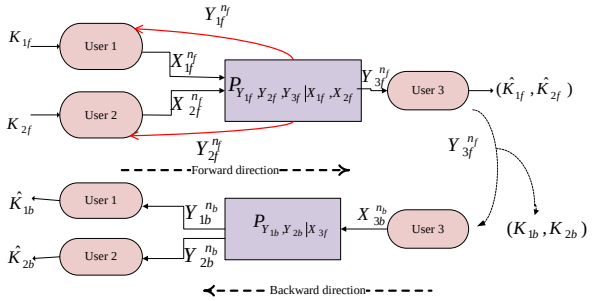

Fig. 1: Secret key sharing using GDMMAC and BC

III. Main Results

Now, the main result of the paper is presented. First, we define:

$$\begin{aligned}
&\alpha \triangleq \tfrac{n_f}{n_f+n_b}, \qquad \bar{\alpha} \triangleq \tfrac{n_b}{n_f+n_b} \\
&R_{1f} \triangleq \alpha[I(T_{1f}; Y_{3f}|T_{2f}) - I(T_{1f}; X_{2f}, Y_{2f}, T_{2fb}|T_{2f})]^+, \\
&R_{1fb} \triangleq \alpha[I(T_{1fb}; X_{1f}, Y_{1f}|T_{1f}) - I(T_{1fb}; X_{2f}, Y_{2f}, T_{2f}, T_{2fb}|T_{1f})]^+, \\
&R_{1b} \triangleq \bar{\alpha}[I(T_{1b}; Y_{1b}) - I(T_{1b}; Y_{2b}, T_{2b})]^+, \\
&R_{2f} \triangleq \alpha[I(T_{2f}; Y_{3f}|T_{1f}) - I(T_{2f}; X_{1f}, Y_{1f}, T_{1fb}|T_{1f})]^+, \\
&R_{2fb} \triangleq \alpha[I(T_{2fb}; X_{2f}, Y_{2f}|T_{2f}) - I(T_{2fb}; X_{1f}, Y_{1f}, T_{1f}, T_{1fb}|T_{2f})]^+, \\
&R_{2b} \triangleq \bar{\alpha}[I(T_{2b}; Y_{2b}) - I(T_{2b}; Y_{1b}, T_{1b})]^+, \\
&R_{12f} \triangleq \alpha[I(T_{1f}, T_{2f}; Y_{3f}) - I(T_{1f}; X_{2f}, Y_{2f}, T_{2fb}|T_{2f}) - \\
&\qquad I(T_{2f}; X_{1f}, Y_{1f}, T_{1fb}|T_{1f})]^+ \qquad (5)
\end{aligned}$$

Theorem 1: In the described setup, all rates in the closure of the convex hull of the set of all key rate pairs (R_1, R_2) that satisfy the following region, are achievable:

$$\begin{cases} R_1 > 0, R_2 > 0 \\ R_1 \leq R_{1f} + R_{1fb} + R_{1b}, \\ R_2 \leq R_{2f} + R_{2fb} + R_{2b}, \\ R_1 + R_2 \leq R_{12f} + R_{1fb} + R_{2fb} + R_{1b} + R_{2b}, \end{cases} \quad (6)$$

subject to the constraints:

$$\begin{aligned}
&n_f I(T_{1fb}; Y_{3f}|X_{1f}, Y_{1f}, T_{1f}) \leq n_b I(X_{3b}; Y_{1b}), \\
&n_f I(T_{2fb}; Y_{3f}|X_{2f}, Y_{2f}, T_{2f}) \leq n_b I(X_{3b}; Y_{2b}), \qquad (7)
\end{aligned}$$

for random variables taking values in sufficiently large finite sets and according to distribution:

$$\begin{aligned}
&p(t_{1f}, t_{2f}, x_{1f}, x_{2f}, y_{1f}, y_{2f}, y_{3f}, t_{1fb}, t_{2fb}, t_{1b}, t_{2b}, x_{3b}, y_{1b}, y_{2b}) = \\
&p(t_{1f})p(t_{2f})p(x_{1f}|t_{1f})p(x_{2f}|t_{2f})p(y_{1f}, y_{2f}, y_{3f}|x_{1f}, x_{2f}) \times \\
&p(t_{1fb}, t_{2fb}|y_{3f})p(t_{1b}, t_{2b})p(x_{3b}|t_{1b}, t_{2b})p(y_{1b}, y_{2b}|x_{3b})
\end{aligned}$$

The proof of Theorem 1 is given in Appendix I. Here, the justification of the above rates is given. As seen in (6), user 1's secret key rate consists of three components. The first term, R_{1f}, is the rate of the key (K_{1f}) that can be generated by user 1 and shared between user 1 and user 3 in the forward direction using only the GDMMAC. The second term, R_{1fb}, is the rate that could be generated from the correlated observations in the forward direction; meaning that the channel outputs of the GDMMAC can be regarded as correlated source observations at the users for secret key generation. For this purpose, user 3 generates K_{1fb} as a function of the received output from GDMMAC for sharing with user 1 and the required information should be sent by user 3 over the BC in the backward direction. The constraints in (7) arise from the fact that the information sent by user 3 should be subject to rate limitations in the backward direction.

Indeed, K_{1fb} is the key that is generated using the correlated observation in the forward direction between users 1 and 3, however, the required information for this goal is transmitted over BC in the backward direction. The third component,R_{1b}, is the rate of the key (K_{1b}) that can be shared between users 1 and 3 using the inherent secrecy of the BC. User 2's key rate and the sum rate can be justified in the same way.

Remark 1: If we cancel the BC by setting $X_{3b} = Y_{1b} = Y_{2b} = T_{1b} = T_{2b} = T_{1fb} = T_{2fb} = \phi$ in Theorem 1, the region reduces to the secrecy rate region of the GDMMAC with two confidential messages as discussed in [5] where the transmitters are eavesdropper with respect to each other.

Remark 2: If we cancel the GDMMAC by setting $T_{1f} = T_{2f} = X_{1f} = X_{2f} = Y_{1f} = Y_{2f} = Y_{3f} = T_{1fb} = T_{2fb} = \phi$ in Theorem 1, the region reduces to the secrecy rate region of the BC with two confidential messages as discussed in [9] where the BC's receivers are eavesdroppers with respect to each other.

Remark 3: If we convert the BC to a noiseless public channel with unlimited capacity in the backward direction by setting $Y_{1b} = Y_{2b}$ and considering $I(X_{3b}; Y_{1b})$ as infinity in Theorem 1, the region reduces to the secret key rate region of the GDMMAC with the backward public channel as in [7].

IV. Special Case

In this section, we derive the secret key capacity region for a special case.

Corollary 1: When the GDMMAC and BC inputs and outputs form Markov chains as $(X_{1f}, X_{2f}) - Y_{2f} - Y_{1f} - Y_{3f}$ and $X_{3b} - Y_{2b} - Y_{1b}$, the secret key capacity region is the set of all rate pairs (R_1, R_2) that satisfy:

$$R_1 \leq I(T_{1fb}; Y_{1f}|Y_{2f}), \qquad R_2 \leq I(X_{3b}; Y_{2b}|Y_{1b}),$$

subject to the constraint:

$$I(T_{1fb}; Y_{3f}|Y_{1f}) \leq I(X_{3b}; Y_{1b}) \tag{8}$$

for random variables taking values in sufficiently large finite sets and according to the distribution:

$$p(x_{1f}, x_{2f}, y_{1f}, y_{2f}, y_{3f}, t_{1fb}, x_{3b}, y_{1b}, y_{2b}) = p(x_{1f})p(x_{2f}) \times p(y_{1f}, y_{2f}, y_{3f}|x_{1f}, x_{2f})p(t_{1fb}|y_{3f})p(x_{3b})p(y_{1b}, y_{2b}|x_{3b})$$

The achievability can be inferred from Theorem 1 by substituting $T_{1f} = T_{2f} = T_{2fb} = T_{1b} = \phi, T_{1fb} = Y_{3f}, T_{2b} = X_{3b}$, and using the above Markov chains. The converse is proved in Appendix II.

In this case, due to Markov chains $(X_{1f}, X_{2f}) - Y_{2f} - Y_{3f}$ and $(X_{1f}, X_{2f}) - Y_{1f} - Y_{3f}$, none of users 1 and 2 can share a secret key with user 3 in the forward direction using just the GDMMAC. However, after the GDMMAC outputs are received in the forward direction by the three users, secret key sharing can be established by user 3 through the noisy BC. For this purpose, user 3 uses the correlation between the received output from the GDMMAC to share a secret key to user 1. The required information is sent to user 1 over the backward BC by user 3 and the rate constraint in (8) is due to this fact. It is evident that no secret key can be shared between user 3 and user 2 using GDMMAC outputs due to Markov chain $Y_{2f} - Y_{1f} - Y_{3f}$. On the other hand, user 3 can agree on a secret key with user 2 exploiting the inherent secrecy of the backward BC which is in favor of user 2 due to Markov chain $X_{3b} - Y_{2b} - Y_{1b}$. With these arguments, achievability of the above key capacity region is justified.

In the following, an example is given to make sense of the secret key sharing in the described framework.

Example 1: Consider binary GDMMAC and BC where all channel inputs and outputs have alphabets $\{0, 1\}$. The GDMMAC and BC input-output relationships at time instant i are according to:

$$Y_{2f,i} = X_{1f,i} \cdot X_{2f,i}, \quad Y_{1f,i} = Y_{2f,i} \oplus E_{1,i}, \quad Y_{3f,i} = Y_{1f,i} \oplus E_{2,i},$$
$$Y_{2b,i} = X_{3b,i} \oplus E_{3,i}, \quad Y_{1b,i} = Y_{2b,i} \oplus E_{4,i},$$

in which $E_{j,i}$ is a binary random variable with the distribution $\Pr(E_{j,i} = 1) = p_j$ where $0 < p_j \leq 0.5$ for $j = 1, .., 4$. The random variables $E_{j,i}$ for $j = 1, .., 4$ are independent of each other. In this example, it can be seen that the GDMMAC and BC inputs and outputs satisfy the same Markov chains as in Corollary 1. Hence, no secret key can be shared just using the GDMMAC in the forward direction. As it was illustrated in the case of Corollary 1, the channel outputs of the GDMMAC can be used by user 3 as source observations and secret key agreement can be established between users 3 and 1 due to the Markov chain $Y_{2f} - Y_{1f} - Y_{3f}$. In fact, the correlation between the noises received by users 1 and 3 from GDMMAC is the potential to generate secrecy. This necessitates sending the required information of the source common randomness from user 3 to user 1 and the backward BC is used to send such information. It should be noted that due to the Markov chain $X_{3b} - Y_{2b} - Y_{1b}$, the backward channel is favorable for user 2 to generate secrecy. Indeed, the backward channel from user 3 to user 1 just serves as a public channel with limited capacity. In this example, we assume fixed value for the parameter p_j for $j = 1, 2, 3$ and investigate the impact of varying p_4 on the secret key capacity region. The secret key capacity region is shown for six values of p_4 in Fig. 2. For $p_4 = 0$, the users 1 and 2 receive same outputs from the BC and so no secret key can be shared between users 2 and 3. In this state, the BC channel can be treated as a public channel with limited capacity from user 3 to the other users to send the required information from user 3 to user 1 in order to key agreement using the channel outputs of GDMMAC. As p_4 increases, the secret key rate between users 3 and 2 would increase as user 1 receives a more noisy output from BC with respect to user 2's received output. On the other hand, increment of p_4 worsen the backward channel from user 3 to 1 and hence, less information can be sent from user 3 to user 1and this results in reducing the secret key rate between users 3 and 1. Therefore, increment of p_4 has a two-side effect on the secret key capacity region. As p_4 reaches to 0.5, the backward channel from user 3 to user 1 becomes a completely random channel and the secret key sharing would be possible just between users 3 and 2.

V. Conclusion

The problem of consecutive secret key sharing over a GDMMAC and BC was studied where users 1 and 2 intended to share secret keys with user 3 while they were eavesdroppers

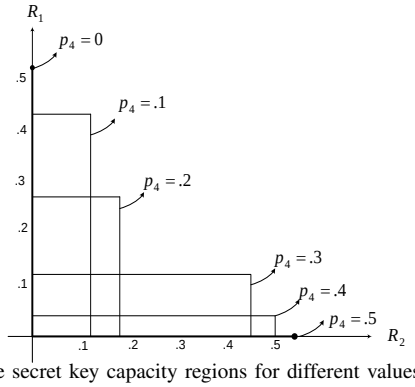

Fig. 2: The secret key capacity regions for different values of noise p_4

with respect to each other. The inner bound of the secret key capacity region was derived. Also, the secret key capacity region was obtained for a special case where the GDMMAC was in favor of user 1 and the BC was in favor of user 2. Also through an example, the bilateral effect of increasing the channel noise from user 3 to user 1 was investigated.

APPENDIX I

Proof of Theorem 1

We fix the distribution to be the same as in Theorem 1. As described in Section II, the secret key sharing is established in two steps; n_f uses of the GDMMAC and n_b uses of the BC. In continue, we describe code construction, encoding and decoding of the two steps separately and then, the security analysis is given.

First, we consider using the GDMMAC. Users 1 and 2 independently generate typical sequences $t_{1f}^{n_f}$ and $t_{2f}^{n_f}$, respectively, each with probability:
$p(t_{1f}^{n_f}) = \prod_{i=1}^{n_f} p(t_{1f,i}), p(t_{2f}^{n_f}) = \prod_{i=1}^{n_f} p(t_{2f,i})$.
The number of the sequences $t_{1f}^{n_f}$ and $t_{2f}^{n_f}$ are $2^{n_f(r_{1f}+r'_{1f})}$ and $2^{n_f(r_{2f}+r'_{2f})}$, respectively, and they are labeled as:

$$t_{1f}^{n_f}(k_{1f}, k'_{1f}), k_{1f} \in \{1, ..., 2^{n_f r_{1f})}\}, k'_{1f} \in \{1, ..., 2^{n_f r'_{1f}}\}$$
$$t_{2f}^{n_f}(k_{2f}, k'_{2f}), k_{2f} \in \{1, ..., 2^{n_f r_{2f})}\}, k'_{2} \in \{1, ..., 2^{n_f r'_{2f}}\}$$

where

r'_{1f}=$I(T_{1f}; T_{2f}, X_{2f}, Y_{2f}, T_{2fb})$−$\varepsilon'$, r'_{2f}=$I(T_{2f}; T_{1f}, X_{1f}, Y_{1f}, T_{1fb})$−$\varepsilon'$,

in which $\varepsilon' > 0$ can be arbitrarily small.

For the first step encoding, when a key index k_{1f} is chosen by user 1, an index k'_{1f} is randomly selected and then for $t_{1f}^{n_f}(k_{1f}, k'_{1f})$, the channel input $x_{1f}^{n_f}$ is sent according to the distribution $p(x_{1f}|t_{1f})$. The same is performed by user 2.

For the first step decoding, user 3 chooses the sequences $t_{1f}^{n_f}$ and $t_{2f}^{n_f}$ which are ε_1-jointly typical with the received $y_{3f}^{n_f}$ where $\varepsilon_1 = \frac{\varepsilon}{8}$. User 3 decodes key pair (k_{1f}, k_{2f}) if $(t_{1f}^{n_f}(k_{1f}, k'_{1f}), t_{2f}^{n_f}(k_{2f}, k'_{2f}), y_{3f}^{n_f}) \in A_{\varepsilon_1}^{n_f}(P_{T_{1f},T_{2f},Y_{3f}})$, when such $(t_{1f}^{n_f}(k_{1f}, k'_{1f}), t_{2f}^{n_f}(k_{2f}, k'_{2f}))$ exists and is unique. Otherwise, it declares error. It can be shown that the decoding error probability of this step is bounded as:

$$P_{e1,f} \leq \varepsilon_1 + 2^{n_f(r_{1f}+r'_{1f}+r_{2f}+r'_{2f}-(I(T_{1f},T_{2f};Y_{3f})-4\varepsilon_1))} + 2^{n_f(r_{1f}+r'_{1f}-(I(T_{1f};T_{2f},Y_{3f})-3\varepsilon_1))} + 2^{n_f(r_{2f}+r'_{2f}-(I(T_{2f};T_{1f},Y_{3f})-3\varepsilon_1))}.$$

If we set:

$$r_{1f} < I(T_{1f}; Y_{3f}|T_{2f}) - I(T_{1f}; X_{2f}, Y_{2f}, T_{2fb}|T_{2f}),$$
$$r_{2f} < I(T_{2f}; Y_{3f}|T_{1f}) - I(T_{2f}; X_{1f}, Y_{1f}, T_{1fb}|T_{1f}),$$
$$r_{1f} + r_{2f} < I(T_{1f}, T_{2f}; Y_{3f}) - I(T_{1f}; X_{2f}, Y_{2f}, T_{2fb}|T_{2f}) - I(T_{2f}; X_{1f}, Y_{1f}, T_{1fb}|T_{1f}),$$

then we have:
$P_{e1,f} \leq \varepsilon_1 + 2^{n_f(-2\varepsilon'+4\varepsilon_1)} + 2^{n_f(-\varepsilon'+3\varepsilon_1)} + 2^{n_f(-\varepsilon'+3\varepsilon_1)}$.
By setting $\varepsilon' > 3\varepsilon_1$, for example $\varepsilon' = 4\varepsilon_1 = \frac{\varepsilon}{2}$, we choose n_f sufficiently large that $2^{n_f(-\varepsilon'+3\varepsilon_1)} \leq \varepsilon_1$, and then $P_{e1,f} \leq 4\varepsilon_1 = \frac{\varepsilon}{2}$.

At the end of the first step, user 3 generates secret keys of the second step as stochastic functions of the channel output y_{3f}^{nf} and sends required information to users 1 and 2 via the backward BC. In this step, user 3 generates $2^{n_f(I(T_{1fb};Y_{3f})+\varepsilon'')}$ and $2^{n_f(I(T_{2fb};Y_{3f})+\varepsilon'')}$ typical sequences t_{1fb}^{nf} and t_{2fb}^{nf}, respectively, each with probability:

$$p(t_{1fb}^{n_f}, t_{2fb}^{n_f}) = \prod_{i=1}^{n_f} p(t_{1fb,i}, t_{2fb,i}).$$

These sequences are labeled using two-layered random binning as:
$t_{1fb}^{n_f}(k_{1fb}, k'_{1fb}, k''_{1fb})$,
k_{1fb}∈$\{1, ..., 2^{n_f r_{1fb}}\}, k'_{1fb}$∈$\{1, ..., 2^{n_f r'_{1fb}}\}, k''_{1fb}$∈$\{1, ..., 2^{n_f r''_{1fb}}\}$,
$t_{2fb}^{n_f}(k_{2fb}, k'_{2fb}, k''_{2fb})$,
k_{2fb}∈$\{1, ..., 2^{n_f r_{2fb}}\}, k'_{2fb}$∈$\{1, ..., 2^{n_f r'_{2fb}}\}, k''_{2fb}$∈$\{1, ..., 2^{n_f r''_{2fb}}\}$,

where:
$r_{1fb} = I(T_{1fb}; X_{1f}, Y_{1f}|T_{1f}) - I(T_{1fb}; X_{2f}, Y_{2f}, T_{2f}, T_{2fb}|T_{1f})$,
$r'_{1fb} = I(T_{1fb}; Y_{3f}|X_{1f}Y_{1f}, T_{1f}) + 2\varepsilon''$,
$r''_{1fb} = I(T_{1fb}; X_{2f}, Y_{2f}, T_{2f}, T_{2fb}, T_{1f}) - \varepsilon''$,
$r_{2fb} = I(T_{2fb}; X_{2f}, Y_{2f}|T_{2f}) - I(T_{2fb}; X_{1f}, Y_{1f}, T_{1f}, T_{1fb}|T_{2f})$,
$r'_{2fb} = I(T_{2fb}; Y_{3f}|X_{2f}, Y_{2f}, T_{2f}) + 2\varepsilon''$,
$r''_{2fb} = I(T_{2fb}; X_{1f}, Y_{1f}, T_{1f}, T_{1fb}, T_{2f}) - \varepsilon''$,
in which ε''>0 can be chosen arbitrarily small. It is obvious that r_{1fb}+r'_{1fb}+r''_{1fb}=$I(T_{1fb}; Y_{3f})$+ε'' and hence, each sequence $t_{1fb}^{n_f}$ can be determined if the indices $(k_{1fb}, k'_{1fb}, k''_{1fb})$ are known and vice versa. The same is true for $t_{2fb}^{n_f}$. Furthermore, user 3 generates typical sequences $t_{1b}^{n_b}$ and t_{2b}^{nb}, each with probability:

$$p(t_{1b}^{n_b}, t_{2b}^{n_b}) = \prod_{i=1}^{n_b} p(t_{1b,i}, t_{2b,i}).$$

The number of sequences $t_{1b}^{n_b}$ and $t_{2b}^{n_b}$ are $2^{n_b(r_{1b}+r'_{1b})}$ and $2^{n_b(r_{2b}+r'_{2b})}$, respectively, and they are labeled as:

$$t_{1b}^{n_b}(k_{1b}, k'_{1b}), k_{1b} \in \{1, ..., 2^{n_b r_{1b})}\}, k'_{1b} \in \{1, ..., 2^{n_b r'_{1b}}\},$$
$$t_{2b}^{n_b}(k_{2b}, k'_{2b}), k_{2b} \in \{1, ..., 2^{n_b r_{2b})}\}, k'_{2b} \in \{1, ..., 2^{n_b r'_{2b}}\},$$

where
$r_{1b} = I(T_{1b}; Y_{1b}) - I(T_{1b}; Y_{2b}, T_{2b}), r'_{1b} = I(T_{1b}; Y_{2b}, T_{2b}) - \varepsilon'''$,
$r_{2b} = I(T_{2b}; Y_{2b}) - I(T_{2b}; Y_{1b}, T_{1b}), r'_{2b} = I(T_{2b}; Y_{1b}, T_{1b}) - \varepsilon'''$,
in which $\varepsilon''' > 0$ can be arbitrarily small.
Due to the inequalities in (7), two functions f_1 and f_2 can be defined as:

$$f_1 : \mathcal{T}_{1b} \to \mathcal{K}'_{1fb}, \qquad f_2 : \mathcal{T}_{2b} \to \mathcal{K}'_{2fb},$$
$$\mathcal{K}'_{1fb} = \{1, ..., 2^{n_f r'_{1fb}}\}, \mathcal{K}'_{2fb} = \{1, ..., 2^{n_f r'_{2fb}}\},$$

where $\mathcal{T}_{1b}$ and $\mathcal{T}_{2b}$ are, respectively, the set of $2^{n_b(I(T_{1b};Y_{1b})-\varepsilon''')}$ and $2^{n_b(I(T_{2b};Y_{2b})-\varepsilon''')}$ codewords $t_{1b}^{n_b}$ and $t_{2b}^{n_b}$. Mapping f_1 is a random partitioning of codewords $t_{1b}^{n_b}$ into $2^{n_f r'_{1fb}}$ equal-sized parts. Elements of part i are labeled as $(\mathcal{T}_{1b})_i$. Mapping f_2 is similarly defined.

Now, we describe the coding scheme of the second step, i.e., using the BC in the backward direction. In this step, user 3 shares two keys with each of users 1 and 2, one derived

from the correlation of GDMMAC outputs at the users and the other derived from the inherent secrecy of the BC. With access to sequence $y_{3f}^{n_f}$, user 3 chooses the codewords $t_{1fb}^{n_f}$ and $t_{2fb}^{n_f}$ which are $\varepsilon''-$jointly typical with $y_{3f}^{n_f}$. Then, he selects the respective index k_{1fb} of the codeword $t_{1fb}^{n_f}$ and k_{2fb} of the codeword $t_{2fb}^{n_f}$ as the second parts of the secret keys with user 1 and user 2, respectively. For these codewords, the respective indices k'_{1fb} and k'_{2fb} are the required information to be sent to user 1 and user 2, respectively, so that each can decode his corresponding key. User 3 encodes (k'_{1fb} and k'_{2fb}) in such a way that he returns $t_{1b}^{n_b}$ and $t_{2b}^{n_b}$, randomly chosen from $(\mathcal{T}_{1b})_{k'_{1fb}}$ and $(\mathcal{T}_{2b})_{k'_{2fb}}$, respectively, using the mappings f_1 and f_2. For the selected $t_{1b}^{n_b}(k_{1b}, k'_{1b})$ and $t_{2b}^{n_b}(k_{2b}, k'_{2b})$, user 3 considers the corresponding indices k_{1b} and k_{2b} as the third parts of the keys to be shared with users 1 and 2, respectively. Then the channel input x_{3b}^{nb} is sent over the BC according to the distributions $p(x_{3b}|t_{1b}, t_{2b})$ by user 3.

For the second step decoding, user 1, first, decodes the sequence $t_{1b}^{n_b}$ and consequently key index k_{1b} by receiving $y_{1b}^{n_b}$. User 1 chooses the sequences $t_{1b}^{n_b}$ which is ε'_1-jointly typical with the received $y_{1b}^{n_b}$ where $\varepsilon'_1 = \frac{\varepsilon}{8}$. User 1 decodes key index k_{1b} if $(t_{1b}^{n_b}(k_{1b}, k'_{1b}), y_{1b}^{n_b}) \in A_{\varepsilon'_1}^{n_b}(P_{T_{1b},Y_{1b}})$, when such $t_{1b}^{n_b}(k_{1b}, k'_{1b})$ exists and is unique. Otherwise, it declares error. It can be seen that the decoding error probability is bounded as:

$$P_{e1,b} \leq \varepsilon'_1 + 2^{-n_b(\varepsilon''' - \varepsilon'_1)},$$

and so, by choosing $\varepsilon''' > \varepsilon'_1$ and considering n_b sufficiently large, it can be bounded as:

$$P_{e1,b} \leq 2\varepsilon'_1 = \frac{\varepsilon}{4}.$$

User 1 considers k_{1b} as the third part of his secret key with user 3. After that, user 1 finds the mapping $(\mathcal{T}_{1b})_i$ of codeword $t_{1b}^{n_b}$ and sets $k'_{1fb} = i$. Now, user 1 decodes sequence $t_{1fb}^{n_f}$ if:
$(t_{1fb}^{n_f}(k_{1fb}{=}i, k''_{1fb}), x_{1f}^{n_f}, y_{1f}^{n_f}, t_{1f}^{n_f}) {\in} A_{\varepsilon''_1}^{n_f}(P_{T_{1fb},X_{1f},Y_{1f}|T_{1f}})$,
when such $t_{1fb}^{n_f}(k_{1fb}, k'_{1fb}, k''_{1fb})$ exists and is unique. Otherwise, it declares error. For $\varepsilon''_1 = \frac{\varepsilon}{8}$, according to Wyner-Ziv problem for multiple sources in [8], it can be seen that the decoding error probability of the sequence $t_{1fb}^{n_f}$ yields as:

$$P_{e1,fb} {\leq} \varepsilon''_1 {+} 2^{n_f(I(T_{1fb};Y_{3f}|X_{1f},Y_{1f},T_{1f}) + \varepsilon''_1 - r'_{1fb})} = \varepsilon''_1 {+} 2^{-n_f(2\varepsilon'' - \varepsilon''_1)}.$$

By choosing $2\varepsilon'' > \varepsilon''_1$ and considering n_f sufficiently large, it can be bounded as $P_{e1,fb} \leq 2\varepsilon''_1 = \frac{\varepsilon}{4}$. After successful decoding, user 1 considers k_{1fb} as the second part of his secret key with user 3. By the above arguments, the secret key triple $(k_{1f}, k_{1fb}, k_{1b})$ can be shared between users 1 and 3 and the total decoding error probabilities is bounded as:

$$P_{e1} < P_{e1,f} + P_{e1,b} + P_{e1,fb} \leq \frac{\varepsilon}{2} + \frac{\varepsilon}{4} + \frac{\varepsilon}{4} = \varepsilon.$$

The same steps can be followed for the secret key triple $(k_{2f}, k_{2fb}, k_{2b})$ between users 2 and 3.

Now, we should check the security conditions of definition 1. We give the proof of (3) and by symmetry, (4) can be deduced. As the keys (K_{1fb}, K_{1b}) are shared in the backward direction, equation (3) can be rewritten as:

$$I(K_{1f}, K_{1fb}, K_{1b}; K_{2f}, X_{2f}^{n_f}, Y_{2f}^{n_f}, Y_{2b}^{n_b}) = \underbrace{I(K_{1f}; K_{2f}, X_{2f}^{n_f}, Y_{2f}^{n_f}, Y_{2b}^{n_b})}_{A} +$$
$$\underbrace{I(K_{1fb}; K_{2f}, X_{2f}^{n_f}, Y_{2f}^{n_f}, Y_{2b}^{n_b} | K_{1f}, K_{1b})}_{B} + \underbrace{I(K_{1b}; K_{2f}, X_{2f}^{n_f}, Y_{2f}^{n_f}, Y_{2b}^{n_b} | K_{1f})}_{C}$$

We analyze the three terms separately. Some Markov chains useful in the security analysis are given below. These Markov chains arise from the coding scheme.

$$(K_{1f}, K_{2f}) - (X_{1f}^{n_f}, X_{2f}^{n_f}) - (Y_{1f}^{n_f}, Y_{2f}^{n_f}, Y_{3f}^{n_f}) \quad (9)$$
$$(X_{1f}^{n_f}, X_{2f}^{n_f}, Y_{1f}^{n_f}, Y_{2f}^{n_f}) - Y_{3f}^{n_f} - (T_{1fb}^{n_f}, T_{2fb}^{n_f}) - (K'_{1fb}, K'_{2fb}) - (T_{1b}^{n_b}, T_{2b}^{n_b}) - (Y_{1b}^{n_b}, Y_{2b}^{n_b}) \quad (10)$$
$$T_{1b}^{n_b}(k_{1b}, k'_{1b}) - T_{2b}^{n_b} - K'_{2fb} - (V_{1f}^{n_f}, X_{1f}^{n_f}, Y_{1f}^{n_f}, V_{2f}^{n_f}, X_{2f}^{n_f}, Y_{2f}^{n_f}) \quad (11)$$
$$T_{2b}^{n_b}(k_{2b}, k'_{2b}) - T_{1b}^{n_b} - K'_{1fb} - (V_{1f}^{n_f}, X_{1f}^{n_f}, Y_{1f}^{n_f}, V_{2f}^{n_f}, X_{2f}^{n_f}, Y_{2f}^{n_f}) \quad (12)$$

For term A, we have:

$$\begin{aligned}
&I(K_{1f}; K_{2f}, X_{2f}^{n_f}, Y_{2f}^{n_f}, Y_{2b}^{n_b}) \overset{(a)}{\leq} I(K_{1f}; T_{2f}^{n_f}, X_{2f}^{n_f}, Y_{2f}^{n_f}, Y_{2b}^{n_b}) \\
&\leq I(K_{1f}; T_{2f}^{n_f}, X_{2f}^{n_f}, Y_{2f}^{n_f}, Y_{2b}^{n_b}, K'_{1fb}, K'_{2fb}) \\
&\overset{(b)}{=} I(K_{1f}; T_{2f}^{n_f}, X_{2f}^{n_f}, Y_{2f}^{n_f}, K'_{1fb}, K'_{2fb}) \\
&\overset{(c)}{\leq} I(K_{1f}; T_{2f}^{n_f}, X_{2f}^{n_f}, Y_{2f}^{n_f}, K'_{1fb}, T_{2fb}^{n_f}) \\
&= I(K_{1f}; T_{2f}^{n_f}, X_{2f}^{n_f}, Y_{2f}^{n_f}, T_{2fb}^{n_f}) + \underbrace{I(K_{1f}; K'_{1fb} | T_{2f}^{n_f}, X_{2f}^{n_f}, Y_{2f}^{n_f}, T_{2fb}^{n_f})}_{I} \\
&= H(K_{1f}) - H(K_{1f} \left| T_{2f}^{n_f}, X_{2f}^{n_f}, Y_{2f}^{n_f}, T_{2fb}^{n_f} \right.) + I \\
&= H(K_{1f}) - H(T_{1f}^{n_f} \left| T_{2f}^{n_f}, X_{2f}^{n_f}, Y_{2f}^{n_f}, T_{2fb}^{n_f} \right.) \\
&+ H(T_{1f}^{n_f} \left| K_{1f}, T_{2f}^{n_f}, X_{2f}^{n_f}, Y_{2f}^{n_f}, T_{2fb}^{n_f} \right.) + I \\
&\overset{(d)}{\leq} H(K_{1f}) - n_f H(T_{1f} | T_{2f}, X_{2f}, Y_{2f}, T_{2fb}) + n_f\varepsilon_2 + n_f\varepsilon_3 + I \\
&\overset{(e)}{\leq} -n_f H(T_{1f} | T_{2f}, Y_{3f}) + n_f\varepsilon_2 + n_f\varepsilon_3 + I \\
&\leq n_f\varepsilon_2 + n_f\varepsilon_3 + I(K'_{1fb}; T_{1f}^{n_f}, T_{2f}^{n_f}, X_{2f}^{n_f}, Y_{2f}^{n_f}, T_{2fb}^{n_f}) \\
&= n_f\varepsilon_2 + n_f\varepsilon_3 + H(K'_{1fb}) - H(K'_{1fb} | T_{1f}^{n_f}, T_{2f}^{n_f}, X_{2f}^{n_f}, Y_{2f}^{n_f}, T_{2fb}^{n_f}) \\
&= n_f\varepsilon_2 + n_f\varepsilon_3 + H(K'_{1fb}) - H(T_{1fb}^{n_f} | T_{1f}^{n_f}, T_{2f}^{n_f}, X_{2f}^{n_f}, Y_{2f}^{n_f}, T_{2fb}^{n_f}) \\
&+ H(K_{1fb}, K''_{1fb} \left| K'_{1fb}, T_{1f}^{n_f}, T_{2f}^{n_f}, X_{2f}^{n_f}, Y_{2f}^{n_f}, T_{2fb}^{n_f} \right.) \\
&\overset{(f)}{\leq} n_f\varepsilon_2 + n_f\varepsilon_3 + H(K'_{1fb}) + H(K_{1fb}) \\
&- n_f H(T_{1fb} | T_{1f}, T_{2f}, X_{2f}, Y_{2f}, T_{2fb}) + n_f\varepsilon_4 + n_f\varepsilon_5 \\
&= n_f\varepsilon_2 + n_f\varepsilon_3 - n_f H(T_{1fb} | T_{1f}, X_{1f}, Y_{1f}) + 2n_f\varepsilon'' + n_f\varepsilon_4 + n_f\varepsilon_5 \\
&\leq n_f\varepsilon_2 + n_f\varepsilon_3 + 2n_f\varepsilon'' + n_f\varepsilon_4 + n_f\varepsilon_5
\end{aligned}$$

In above equations, (a) follows from the fact that index k_{2f} is one of the indices of $t_{2f}^{n_f}$. (b) is due to Markov chain (10) and (c) follows from the fact that index k'_{2fb} is one of the indices of $t_{2fb}^{n_f}$. To prove (d), the same approach as lemma 2 and 3 in [9] can be exploited to show $n_f H(T_{1f}|T_{2f}, X_{2f}, Y_{2f}, T_{2fb}) \leq H(T_{1f}^{n_f}|T_{2f}^{n_f}, X_{2f}^{n_f}, Y_{2f}^{n_f}, T_{2fb}^{n_f}) + n_f\varepsilon_2$ and $H(T_{1f}^{n_f}|K_{1f}, T_{2f}^{n_f}, X_{2f}^{n_f}, Y_{2f}^{n_f}, T_{2fb}^{n_f}) \leq n_f\varepsilon$. (e) is deduced from the reliable decoding condition of k_{1f}. (f) can be deduced from the same approaches as (d).

For term B, we have:

$$\begin{aligned}
&I(K_{1fb}; K_{2f}, X_{2f}^{n_f}, Y_{2f}^{n_f}, Y_{2b}^{n_b} | K_{1f}, K_{1b}) \\
&\leq I(K_{1fb}; K'_{1fb}, K'_{2fb}, T_{1f}^{n_f}, T_{2f}^{n_f}, T_{1b}^{n_f}, X_{2f}^{n_f}, Y_{2f}^{n_f}, Y_{2b}^{n_b}) \\
&\overset{(a)}{=} I(K_{1fb}; K'_{1fb}, K'_{2fb}, T_{1f}^{n_f}, T_{2f}^{n_f}, X_{2f}^{n_f}, Y_{2f}^{n_f}) \\
&\leq I(K_{1fb}; K'_{1fb}, T_{2fb}^{n_f}, T_{1f}^{n_f}, T_{2f}^{n_f}, X_{2f}^{n_f}, Y_{2f}^{n_f}) \\
&= H(K_{1fb}) - H(K_{1fb} \left| K'_{1fb}, T_{2fb}^{n_f}, T_{1f}^{n_f}, T_{2f}^{n_f}, X_{2f}^{n_f}, Y_{2f}^{n_f} \right.) \\
&\leq H(K_{1fb}) + H(K'_{1fb}) - H(T_{1fb}^{n_f} \left| T_{2fb}^{n_f}, T_{1f}^{n_f}, T_{2f}^{n_f}, X_{2f}^{n_f}, Y_{2f}^{n_f} \right.) \\
&+ H(T_{1fb}^{n_f} \left| K_{1fb}, K'_{1fb}, T_{2fb}^{n_f}, T_{1f}^{n_f}, T_{2f}^{n_f}, X_{2f}^{n_f}, Y_{2f}^{n_f} \right.) \\
&\overset{(b)}{\leq} H(K_{1fb}) + H(K'_{1fb}) - n_f H(T_{1fb}|T_{1f}, T_{2f}, X_{2f}, Y_{2f}, T_{2fb}) + n_f\varepsilon_4 + n_f\varepsilon_5
\end{aligned}$$

$$= -n_f H(T_{1fb}\Big|T_{1f}, X_{1f}, Y_{1f}) + 2n_f\varepsilon'' + n_f\varepsilon_4 + n_f\varepsilon_5$$
$$\leq 2n_f\varepsilon'' + n_f\varepsilon_4 + n_f\varepsilon_5$$

In the above equations, (a) can be deduced from the Markov chain (10) and (b) from the same arguments in term A.

For term C, we have:

$$I(K_{1b}; K_{2f}, X_{2f}^{n_f}, Y_{2f}^{n_f}, Y_{2b}^{n_b}|K_{1f})$$
$$\leq I(K_{1b}; K_{1f}, K_{2f}, X_{2f}^{n_f}, Y_{2f}^{n_f}, Y_{2b}^{n_b})$$
$$\leq I(K_{1b}; V_{1f}^{n_f}, V_{2f}^{n_f}, X_{2f}^{n_f}, Y_{2f}^{n_f}, Y_{2b}^{n_b}, K'_{2fb})$$
$$\overset{(a)}{=} I(K_{1b}; Y_{2b}^{n_b}, K'_{2fb}) \leq I(K_{1b}; Y_{2b}^{n_b}, K'_{2fb}, T_{2b}^{n_f})$$
$$\overset{(b)}{=} I(K_{1b}; Y_{2b}^{n_b}, T_{2b}^{n_f}) = H(K_{1b}) - H(K_{1b}\Big|Y_{2b}^{n_b}, T_{2b}^{n_f})$$
$$= H(K_{1b}) - H(T_{1b}^{n_f}\Big|Y_{2b}^{n_b}, T_{2b}^{n_f}) + H(T_{1b}^{n_f}\Big|K_{1b}, Y_{2b}^{n_b}, T_{2b}^{n_f})$$
$$\overset{(c)}{\leq} H(K_{1b}) - n_b H(T_{1b}\big|Y_{2b}, T_{2b}) + n_b\varepsilon_6 + n_b\varepsilon_7$$
$$= -n_b H(T_{1b}\big|Y_{1b}) + n_b\varepsilon_6 + n_b\varepsilon_7 \leq n_b\varepsilon_6 + n_b\varepsilon_7$$

In the above equations, (a) and (b) can be deduced from the Markov chain (11). To prove (b), the same approach as lemma 2 and 3 in [9] is exploited to show $n_b H(T_{1b}|Y_{2b}, T_{2b}) \leq H(T_{1b}^{n_f}|Y_{2b}^{n_b}, T_{2b}^{n_f}) + n_b\varepsilon_6$ and $H(T_{1b}^{n_f}|K_{1b}, Y_{2b}^{n_b}, T_{2b}^{n_f}) \leq n_b\varepsilon_7$. By substituting $\varepsilon'' = \frac{\varepsilon}{12}, \varepsilon_i = \frac{\varepsilon}{9}, \varepsilon_j = \frac{\varepsilon}{2}$ for $i = 2, .., 5$ and $j = 6, 7$, the security condition (3) is satisfied as:

$$I(K_{1f}, K_{1fb}, K_{1b}; K_{2f}, X_{2f}^{n_f}, Y_{2f}^{n_f}, Y_{2b}^{n_b}) \leq (n_f + n_b)\varepsilon.$$

To show that the total rate of user 1's secret key is the sum of the rates r_{1f}, r_{1fb} and r_{1b}, we should prove the independency of the keys. When analyzing terms B and C of the security condition, we show that:

$$I(K_{1fb}; K_{1f}, K_{1fb}) \leq I(K_{1fb}; K_{1f}, K_{2f}, K_{1fb}, X_{2f}^{n_f}, Y_{2f}^{n_f}, Y_{2b}^{n_b})$$
$$\leq 2n_f\varepsilon'' + n_f\varepsilon_4 + n_f\varepsilon_5$$
$$I(K_{1b}; K_{1f}) \leq I(K_{1b}; K_{1f}, K_{2f}, X_{2f}^{n_f}, Y_{2f}^{n_f}, Y_{2b}^{n_b}) \leq n_b\varepsilon_6 + n_b\varepsilon_7$$

and hence:

$$H(K_{1f}, K_{1fb}, K_{1b}) \geq H(K_{1f}) + H(K_{1fb}) + H(K_{1b}) -$$
$$(2n_f\varepsilon'' + n_f\varepsilon_4 + n_f\varepsilon_5 + n_b\varepsilon_6 + n_b\varepsilon_7)$$
$$\geq H(K_{1f}) + H(K_{1fb}) + H(K_{1b}) - (n_f + n_b)\varepsilon,$$

and this completes the proof of theorem 1.

It should be noted that in the code construction of the second step, we implicitly assume $I(T_{1b}; Y_{1b}) \geq I(T_{1b}; Y_{2b}, T_{2b})$. In the case where $I(T_{1b}; Y_{1b}) < I(T_{1b}; Y_{2b}, T_{2b})$, user 3 randomly maps k'_{1fb} into a space with $2^{n_b(I(T_{1b};Y_{1b})-\varepsilon'_1)}$ elements and no secret key is chosen as k_{1b}. The same is true about user 2's codebook.

APPENDIX II

Proof of the converse in Corollary 2

To derive the outer bound in Corollary 1, it is assumed that the keys are produced in two steps as discribed in Section 2.

Applying Fano's inequality to the corresponding keys at the users, for an arbitrary small$\varepsilon > 0$, we obtain:

$$H(K_{1f}, K_{2f}|Y_{3f}^{n_f}) \leq n_f(\tfrac{h(\varepsilon)}{n_f} + \varepsilon\log(|\mathcal{K}_{1f}|\,|\mathcal{K}_{2f}| - 1)) \triangleq n_f\varepsilon_1,$$
$$H(K_{1b}|K_{1f}, X_{1f}^{n_f}, Y_{1f}^{n_f}, Y_{1b}^{n_b}) \leq n_b(\tfrac{h(\varepsilon)}{n_b} + \varepsilon(\log|\mathcal{K}_{1b}| - 1)) \triangleq n_b\varepsilon_2,$$
$$H(K_{2b}|K_{2f}, X_{2f}^{n_f}, Y_{2}^{n_f}, Y_{2b}^{n_b}) \leq n_b(\tfrac{h(\varepsilon)}{n_b} + \varepsilon(\log|\mathcal{K}_{2b}| - 1)) \triangleq n_b\varepsilon_3,$$

where $|\mathcal{K}_{1f}|$ is the cardinality of key set $\mathcal{K}_{1f}$ and $\varepsilon_i \to 0$ if $\varepsilon \to 0$ for $i = 1, 2, 3$.

Now, we show that for the secret keys satisfying above reliability conditions and the security conditions (3) and (4) in Definition 1, there exist random variables according to the distribution of Corollary 1 satisfying the mentioned relations. We prove the outer bound of R_1. The outer bound of R_2 can be deduced using the same approaches. Before launching proof, Markov chains are given which are useful in continue:

$$(K_{1f}, K_{2f}) - (X_{1f}^{n_f}, X_{2f}^{n_f}) - Y_{2f}^{n_f} - Y_{1f}^{n_f} - Y_{3f}^{n_f} - (K_{1b}, K_{2b}, X_{3b}^{n_b}, Y_{2b}^{n_b}, Y_{1b}^{n_b}) \quad (13)$$

$$(K_{1b}, K_{2b}) - X_{3b}^{n_b} - Y_{2b}^{n_b} - Y_{1b}^{n_b} \quad (14)$$

It is defined:

$$\varepsilon' = \frac{2(n_f + n_b)\varepsilon + n_f\varepsilon_1 + n_b\varepsilon_2}{(n_f + n_b)}.$$

We have:

$$(n_f + n_b)R_1 \leq H(K_{1f}, K_{1b}) + (n_f + n_b)\varepsilon$$
$$\overset{(a)}{\leq} H(K_{1f}, K_{1b}|K_{2f}, X_{2f}^{n_f}, Y_{2f}^{n_f}, Y_{2b}^{n_b}) + 2(n_f + n_b)\varepsilon$$
$$\overset{(b)}{\leq} H(K_{1f}|K_{2f}, X_{2f}^{n_f}, Y_{2f}^{n_f}, Y_{2b}^{n_b}) + H(K_{1b}|K_{1f}, K_{2f}, X_{2f}^{n_f}, Y_{2f}^{n_f}, Y_{2b}^{n_b})$$
$$- H(K_{1f}|K_{2f}, Y_{3f}^{n_f}) - H(K_{1b}|K_{1f}, X_{1f}^{n_f}, Y_{1f}^{n_f}, Y_{1b}^{n_b}) + (n_f + n_b)\varepsilon'$$
$$\overset{(c)}{\leq} I(K_{1f}; Y_{3f}^{n_f}|K_{2f}, X_{2f}^{n_f}, Y_{2f}^{n_f}) +$$
$$I(K_{1b}; X_{1f}^{n_f}, Y_{1f}^{n_f}|K_{1f}, K_{2f}, X_{2f}^{n_f}, Y_{2f}^{n_f}, Y_{1b}^{n_b}) + (n_f + n_b)\varepsilon'$$
$$\overset{(d)}{\leq} I(X_{1f}^{n_f}; Y_{3f}^{n_f}|X_{2f}^{n_f}, Y_{2f}^{n_f}) +$$
$$I(K_{1b}, Y_{1b}^{n_b}; X_{1f}^{n_f}, Y_{1f}^{n_f}|K_{1f}, K_{2f}, X_{2f}^{n_f}, Y_{2f}^{n_f}) + (n_f + n_b)\varepsilon'$$
$$\overset{(e)}{=} 0 + I(K_{1b}, Y_{1b}^{n_b}; Y_{1f}^{n_f}|Y_{2f}^{n_f}) + (n_f + n_b)\varepsilon'$$
$$\leq \textstyle\sum_{i=1}^{n_f} I(K_{1b}, Y_{1b}^{n_b}, Y_{1f,1}^{i-1}; Y_{1f,i}|Y_{2f}^{n_f}) + (n_f + n_b)\varepsilon'$$
$$\leq \textstyle\sum_{i=1}^{n_f} I(K_{1b}, Y_{1b}^{n_b}, Y_{1f,1}^{i-1}, Y_{3f,i+1}^{n_f}; Y_{1f,i}|Y_{2f}^{n_f}) + (n_f + n_b)\varepsilon'$$
$$\overset{(f)}{=} \textstyle\sum_{i=1}^{n_f} I(K_{1b}, Y_{1b}^{n_b}, Y_{1f,1}^{i-1}, Y_{3f,i+1}^{n_f}; Y_{1f,i}|Y_{2f,i}) + (n_f + n_b)\varepsilon'$$
$$\overset{(g)}{=} n_f I(T_{1fb,Q}; Y_{1f,Q}|Y_{2f,Q}) + (n_f + n_b)\varepsilon'$$

where (a) results from the security conditions, (b) from Fano's inequalities, (c) from the Markov chain (14), (d) and (e) from the Markov chain (13), (f) from the combination of the memoryless property and Markov chain (13), (g) from the definition of the random variable $T_{1fb,i} \triangleq K_{1b}, Y_{1b}^{n_b}, Y_{1f,1}^{i-1}, Y_{3f,i+1}^{n_f}$ and considering the random variable Q which is uniformly distributed on $\{1, 2, ..., N\}$.

With the same approach, it can be shown that:

$$(n_f + n_b)R_2 \leq n_b I(X_{3b}; Y_{2b}\,|Y_{1b}) + 2(n_f + n_b)\varepsilon + n_f\varepsilon_1 + n_b\varepsilon_3.$$

In the following, the rate constraint in corollary 1 is proved.

$$n_b I(X_{3b}; Y_{1b}) \geq I(X_{3b}^{n_b}; Y_{1b}^{n_b}) \geq I(Y_{3f}^{n_f}; Y_{1b}^{n_b})$$
$$\overset{(a)}{\geq} I(Y_{3f}^{n_f}; Y_{1b}^{n_b}) + H(K_{1b}|K_{1f}, X_{1f}^{n_f}, Y_{1f}^{n_f}, Y_{1b}^{n_b}) - n_b\varepsilon_2$$
$$\overset{(b)}{=} I(Y_{3f}^{n_f}; Y_{1b}^{n_b}) + H(K_{1b}|Y_{1f}^{n_f}, Y_{1b}^{n_b}) - n_b\varepsilon_2$$
$$\geq I(Y_{3f}^{n_f}; Y_{1b}^{n_b}, K_{1b}) - I(Y_{1f}^{n_f}; Y_{1b}^{n_b}, K_{1b}) - n_b\varepsilon_2$$
$$\overset{(c)}{=} I(K_{1b}, Y_{1b}^{n_b}; Y_{3f}^{n_f}|Y_{1f}^{n_f}) - n_b\varepsilon_2$$
$$= \textstyle\sum_{i=1}^{n_f} I(K_{1b}, Y_{1b}^{n_b}; Y_{3f,i}|Y_{1f}^{n_f}, Y_{3f,i+1}^{n_f}) - n_b\varepsilon_2$$
$$\overset{(d)}{=} \textstyle\sum_{i=1}^{n_f} H(Y_{3f,i}|Y_{1f,i}) - \sum_{i=1}^{n_f} H(Y_{3f,i}|Y_{1f}^{n_f}, Y_{3f,i+1}^{n_f}, K_{1b}, Y_{1b}^{n_b}) - n_b\varepsilon_2$$
$$= \textstyle\sum_{i=1}^{n_f} I(K_{1b}, Y_{1b}^{n_b}, Y_{1f,1}^{i-1}, Y_{3f,i+1}^{n_f}; Y_{3f,i}\,|Y_{1f,i}) - n_b\varepsilon_2$$
$$= n_f I(T_{1fb,Q}; Y_{3f,Q}|Y_{1f,Q}) - n_b\varepsilon_2$$

where (a) results from Fano's inequality, (b) and (c) from the Markov chain (13) and (d) from the combination of the memoryless property and Markov chain (13).

REFERENCES

[1] R. Ahlswede and I. Csiszar, "Common randomness in information theory and cryptography, part I: Secret sharing," *IEEE Trans. Inf. Theory*, vol. 39, no. 4, pp. 1121–1132, Jul. 1993.

[2] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 733–742, May 1993.

[3] T. M. Cover and J. A. Thomas, Elements of Information Theory. New York: John Wiley & Sons, 2nd Edition, 2006.

[4] H.Ahmadi, R. Safavi-Naini, "Secret key establishment over a pair of independent broadcast channels," *IEEE Int. Symp. Inf. Theory and its Application (ISITA)*, Taichung, Taiwan, pp. 185-190, Oct. 2011.

[5] Y. Liang and V. Poor, "Multiple access channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 54, no. 3, pp. 976-1002, Mar. 2008.

[6] S. Salimi, M. Salmasizadeh, M. R. Aref, Jovan Dj Golic, "Key Agreement over Multiple Access Channel," *IEEE Trans. on Information Forensics and Security*, vol. 6, Issue 3, pp. 775-790, Sep. 2011.

[7] S. Salimi, M. Salmasizadeh, M. R. Aref, "Key Agreement over Multiple Access Channel Using Feedback Channel," *IEEE Int. Symp. Inf. Theory (ISIT)*, Saint Petersburg, Russia, pp. 1936-1940, Aug. 2011.

[8] M. Gastpar, "The Wyner-Ziv problem with multiple sources," *IEEE Trans. Inf. Theory*, vol. 50, no. 11, pp. 2762 - 2768, Nov. 2004.

[9] R. Liu, I. Maric, P. Spasojevic, R. D. Yate, "Discrete memoryless interference and broadcast channels with confidential messages: Secrecy rate regions," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 1–14, Jun. 2008.

[10] E. Ekrem and S. Ulukus, "Effects of Cooperation on the Secrecy of Multiple Access Channels with Generalized Feedback," *Annual Conf. on Information Sciences and Systems (CISS)*, Princeton, NJ , pp. 791 – 796, March 2008.